OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

17 NOV 1999

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
ATTENTION: SERVICE ACQUISITION EXECUTIVES
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL COMMUNICATIONS & INTELLIGENCE)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR FOR FORCE STRUCTURE, RESOURCES & ASSESSMENT, JOINT STAFF (J-8)
DIRECTOR, DEVELOPMENTAL TEST AND EVALUATION, S&TS
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
DIRECTOR, NAVY TEST & EVALUATION & TECHNOLOGY REQUIREMENTS
DIRECTOR, AIR FORCE TEST & EVALUATION

SUBJECT: Policy for Operational Test and Evaluation of Information Assurance

The attached Policy for Operational Test and Evaluation of Information Assurance is effective immediately. The Department of Defense faces widespread threats in the form of information attacks to the information superiority upon which so much of our current and future military capability depends. It will support Joint Vision 2010 by protecting vulnerable military systems from information warfare attack. The policy also comes at an opportune time since new Congressional language in the FY2000 DoD Appropriations Bill mandates information assurance testing in Independent Operational Test and Evaluation.

This policy has undergone extensive coordination over the past two years via several workshops with all of the Services and information assurance experts. I have insured that the Service recommended changes in earlier versions have been satisfactorily incorporated, and have been accepted by the workshop participants in its current form. The policy has been crafted to maximize the use of existing processes and information in order to reduce the burden on all involved parties to the greatest extent practicable. I will continue to work with the Services and various agencies on efforts to better define and standardize the metrics to be used in testing and evaluating systems' information assurance levels and capabilities. I welcome your continued participation and support in this important endeavor.

My point of contact for this effort is COL Terry Mitchell, who can be reached at (703) 681-1440 or DSN 761-1440. His email address is tmitchell@dote.osd.mil.

Philip E. Coyle
Director

cc:

ATEC
OPTEVFOR
AFOTEC
MCOTEA
JITC
JOINT STAFF J-6

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

Policy on Operational Test and Evaluation of Information Assurance

This document establishes the supporting policy for Operational Test and Evaluation (OT&E) of Information Assurance (IA) of all Director, Operational Test and Evaluation (DOT&E) oversight programs, including weapon systems; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems; and information systems.

BACKGROUND

Information superiority is one of the key goals for Joint Vision 2010. Widespread use of modern information technology has led to a critical dependence of operations on information that is vulnerable to attack. This vulnerability needs to be addressed throughout a new system's development and testing phases. Formalized operational evaluation of all systems' IA capability is required to ensure that users are aware of a system's vulnerabilities.

Applicable DoD directives, instructions, and regulations include DoD Regulation 5000.2-R, DoD Directive (DoDD) S3600.1, DoDD 5200.28, as well as the supplement to DoDD 5200.28, and DoD Instruction (DoDI) 5200.40.

DoD Regulation 5000.2-R discusses IA in Section 4.4.6 and states, "Information assurance requirements shall ... ensure availability, integrity, authentication, confidentiality, and non-repudiation of critical program technology and information. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. Information assurance requirements shall be established and maintained throughout the acquisition life-cycle for all ACAT I programs and others as applicable." DoDD S3600.1 is the overarching classified document on Information Operations. DoDD 5200.28 discusses Computer Security for Automated Information Systems in terms of the old Orange Book/Rainbow series criteria. DODI 5200.40, entitled DoD Information Technology Security Certification and Accreditation Process (DITSCAP), provides useful supporting information and structure. None of these documents address operational testing. This memorandum supplements these documents by formulating OT&E policy for IA.

APPLICABILITY AND SCOPE

This policy applies to all DOT&E oversight programs that are dependent on external information sources or that provide information to other DoD systems. This policy applies to all new development programs and all programs that have not reached Milestone III prior to the effective date of this policy. OTAs are encouraged to use this policy for non-oversight programs whenever practicable.

DEFINITIONS

Terms used in this policy are defined in Appendix A.

IMPLEMENTATION

A four-step IA OT&E process is shown in Figure 1 and described below.

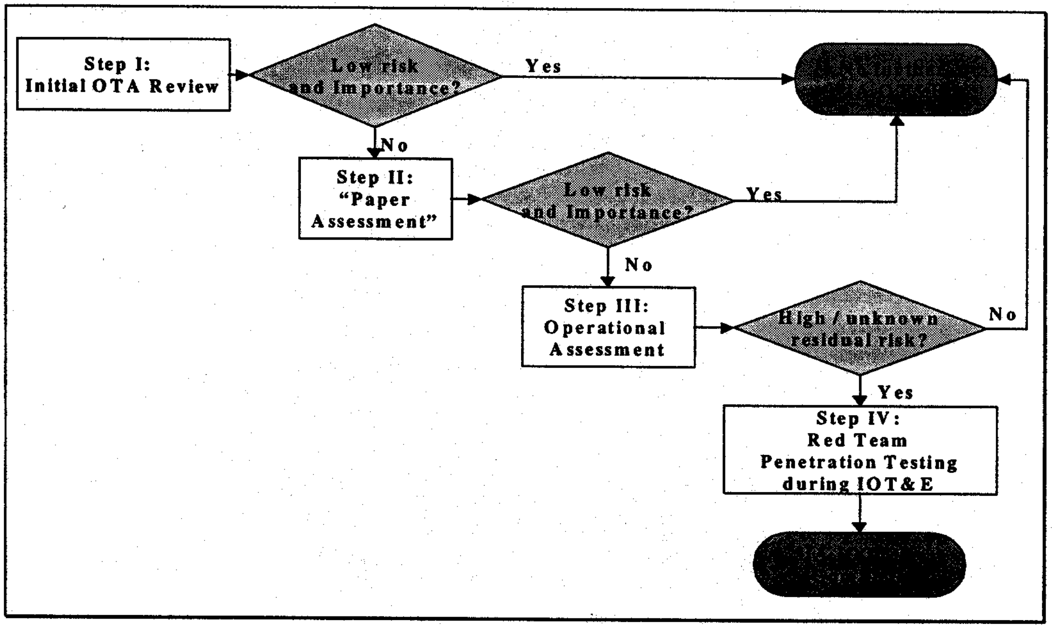

Figure 1: IA OT&E Process

Step I: Requirements, Threat, and Test Documentation Review.

For all DOT&E oversight programs, the OTAs, with the assistance and concurrence of DOT&E, will ensure that an initial document review of each program and system is conducted to determine the relevance of IA testing based on requirements, assessed vulnerabilities, and the importance of the program functions and missions. This review should be undertaken at the earliest possible phase of system development led by the acquisition program manager in cooperation with the OTAs, the users, and those organizations that will be involved in the design, testing, and certification process of the system. This review should leverage all available information including IA mission requirements, Defense Intelligence Agency (DIA) or Service-provided threat assessments, program manager and user-provided relevant information, and expert judgments as necessary.

For those programs falling under the DITSCAP, direct coordination with the System Security Authorization Agreement (SSAA) signatories throughout the acquisition cycle is necessary to minimize duplicative effort by the OTAs. Opportunities to meet operational requirements through concurrent testing will be maximized, particularly in

DITSCAP Phase 2 Vulnerability Assessments and Phase 3 Security Test and Evaluation and Penetration Testing.

If vulnerabilities are assessed to be minimal, then the program can be waived from further IA OT&E by mutual agreement of DOT&E and the OTAs. Vulnerabilities will be detailed in appropriate program documentation, preferably the Test and Evaluation Master Plans (TEMPs) and the operational test plans or their annexes. For the programs that have not been waived from operational IA testing, the TEMPs and test plans should include at least one operational issue or sub-issue for the evaluation of IA vulnerability. The operational test plan will specify IA test concepts. The TEMPs should reference a System Threat Assessment Report (STAR) or a pertinent document for threat assessment. The Joint Staff or responsible Service component is expected to provide specific IA requirements, as required by DoD 5000.2-R, for all new Operational Requirements Documents (ORDs)/Joint ORDs (JORDs).

Step II: Test Strategy Development.

For those programs that have not been waived in the Step I review, a paper vulnerability assessment will take place as part of the normal test strategy development process using experts, program manager personnel, OTA representatives, users, and others as needed to define the degree to which operational IA testing is warranted. This step will also identify programs that could stop at this level of operational IA assessment and would not be required to proceed to Steps III and IV below. DOT&E will not approve TEMPs and test plans for oversight programs unless they contain a well-defined strategy for addressing IA concerns, adequate resources, and appropriate measures against which to test stated requirements. Those programs with IA OT&E waivers will note this in their TEMP and test plan.

Step III: Review of Information Assurance Development Test and Evaluation (DT&E) and Computer Security Certification Results Prior to Entry into OT&E.

Based on the Step II assessment, for systems that are deemed to possess potentially high or unknown residual IA risk, the OTAs will examine DT&E and DITSCAP data, including any concurrent operational assessments that may have already occurred, in judging the operational effectiveness of that system. If the DT&E, DITSCAP and possible operational assessment data show that the vulnerabilities are not serious, then the system will not be subject to penetration testing during IOT&E. Otherwise, the system will be required to conduct penetration testing during IOT&E as described in Step IV below. The DT&E/DITSCAP data will be used during the operational test readiness review in judging whether the system is ready to enter IOT&E. All unresolved deficiencies uncovered in any IA assessment will be examined for possible evaluation during the conduct of IOT&E.

Step IV: Evaluation of Information Assurance Vulnerabilities During Operational Test.

Those programs that have undergone Steps I, II, and III, and are still judged to have high or unknown vulnerabilities will be subject to field penetration testing by a Red

Team as part of the IOT&E. The IOT&E will include a realistic operational environment, and the Red Team capabilities will be commensurate with the threat and expected risks for that program. The IOT&E test plans should define the IA evaluation, with supporting measures. DITSCAP Phase III Penetration Testing and IOT&E may be conducted concurrently, provided that operational test objectives are not compromised using this approach.

Documentation

This policy guidance on IA OT&E will be transitioned to DoDD 5000.2. In concert with ASD(C3I), OTAs, and others as appropriate, DOT&E will further develop IA OT&E guidelines to assist in the evaluation and assessment of systems including metrics. Finally, DOT&E will report IA effectiveness in oversight programs as a regular item in the DOT&E Annual Report and the Beyond Low-Rate Initial Production (B-LRIP) report to the Secretary of Defense and Congress.

EFFECTIVE DATE

This policy is effective immediately.

Philip E. Coyle
Director

cc:

OPTEC
OPTEVFOR
AFOTEC
MCOTEA
JITC
JOINT STAFF J-6

APPENDIX A
DEFINITIONS

1. **Assessment:** An effort to gain insight into system capabilities and limitations. May be conducted in many ways including a paper analysis, laboratory type testing, or even through limited testing with operationally representative users and equipment in an operational environment. Not sufficiently rigorous in and of itself to allow a determination of effectiveness and suitability to be made for purposes of operational testing.
2. **Detect:** To discover threat activity within information systems, such as initial intrusions, during the threat activity or post-activity. Providing prompt awareness and standardized reporting of attacks and other anomalous external or internal system and network activity.
3. **DoD Information Technology Security Certification and Accreditation Process (DITSCAP):** The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security.
4. **Importance:** A subjective assessment of the significance of a system's capability and the consequences of the loss of that capability.
5. **Information Assurance (IA):** Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. *(fm JP3-13)*
6. **Information Operations (IO):** Actions taken to affect adversary information and information systems while defending one's own information and information systems. *(fm JP3-13)*
7. **Information System:** The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. *(fm JP3-13)*
8. **Information Warfare (IW):** Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over s specific adversary or adversaries. *(fm JP3-13)*
9. **Protect:** To keep information systems away from intentional, unintentional, and natural threats; (1) preclude an adversary from gaining access to information for the purpose of destroying, corrupting, or manipulating such information; or (2) deny use of information systems to access, manipulate, and transmit mission-essential information.
10. **React:** To respond to threat activity within information systems, when detected, and mitigate the consequences by taking appropriate action to incidents that threaten information and information systems.
11. **Red Team:** A group of people duly authorized to conduct attacks against friendly information systems, under prescribed conditions, for the purpose of revealing the capabilities and limitations of the Information Assurance posture of a system under test. For purposes of operational testing, the Red Team will operate in as operationally realistic an environment as feasible and will conduct its operations in accordance with the approved operational test plan.
12. **Risk:** A subjective assessment comprising the importance of a system's IA vulnerabilities, and the likelihood that these vulnerabilities can and will be exploited.